FORM PTO-1390 US DEPARTMENT OF COMMERCE REV. 5-93PATENT AND TRADEMARK OFFICE **TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371**		ATTORNEYS DOCKET NUMBER **P01,0142** U.S. APPLICATION NO. (if known, see 37 CFR 1.5) 09/831046
INTERNATIONAL APPLICATION NO. **PCT/DE99/03262**	INTERNATIONAL FILING DATE **11 OCTOBER 1999**	PRIORITY DATE CLAIMED **03 NOVEMBER 1998**

TITLE OF INVENTION
METHOD AND ARRANGEMENT FOR AUTHENTICATING A FIRST ENTITY AND A SECOND ENTITY

APPLICANT(S) FOR DO/EO/US
Martin EUCHNER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. □ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. □ has been transmitted by the International Bureau.
   c. □ is ~~not~~ required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2).

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))
   a. □ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. □ have been transmitted by the International Bureau.
   c. □ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. □ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; **(PTO 1449, Prior Art, Search Report, 11 References)**.

12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included.
    (SEE ATTACHED ENVELOPE)

13. ☒ Amendment "A" Prior to Action and Appendix "A".
    □ A SECOND or SUBSEQUENT preliminary amendment.

14. ☒ A substitute specification and substitute specification mark-up.

15. □ A change of address letter attached to the Declaration.

16. ☒ Other items or information:
    a. ☒ Submission of Drawings
    b. ☒ EXPRESS MAIL #EL 843728288 US dated May 3, 2001

U.S. APPLICATION NO. (If known, see 37 C F R 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/831046	PCT/DE99/03262	P01,0142

17. ☒ The following fees are submitted:

				CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO $860.00 International preliminary examination fee paid to USPTO (37 C.F.R 1.482) $690 00 No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C F R. 1.445(a)(2) $710.00 Neither international preliminary examination fee (37 C.F.R. 1 482) nor international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO $1000.00 International preliminary examination fee paid to USPTO (37 C F R. 1 482) and all claims satisfied provisions of PCT Article 33(2)-(4) $ 100 00					
ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 860.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 C F.R. 1 492(e)).				$	
Claims	Number Filed	Number Extra	Rate		
Total Claims	10 - 20 =	0	X $ 18.00	$	
Independent Claims	03 - 3 =	0	X $ 80.00	$	
Multiple Dependent Claims			$270.00 +	$	
TOTAL OF ABOVE CALCULATIONS =				$ 860.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)				$	
SUBTOTAL =				$ 860.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)) +				$	
TOTAL NATIONAL FEE =				$ 860.00	
Fee for recording the enclosed assignment (37 C.F R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3 28, 3.31) $40 00 per property +					
TOTAL FEES ENCLOSED =				$ 860.00	
				Amount to be refunded	$
				charged	$

a. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. ____________ in the amount of $ ________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1519. **A duplicate copy of this sheet is enclosed.**

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473

CUSTOMER NUMBER 26574

Mark Bergner

SIGNATURE - MARK BERGNER (Reg. No. 45,877)

Date: May 3, 2001

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

PRELIMINARY AMENDMENT A
PRIOR TO ACTION

APPLICANT(S):	Martin EUCHNER
ATTORNEY DOCKET NO.:	P01,0142
INTERNATIONAL APPLICATION NO:	PCT/DE99/03262
INTERNATIONAL FILING DATE:	11 OCTOBER 1999

INVENTION: METHOD AND ARRANGEMENT FOR AUTHENTICATING A FIRST ENTITY AND A SECOND ENTITY

Assistant Commissioner for Patents,
Washington D.C. 20231

Sir:

Applicants herewith amend the above-referenced PCT application, and request entry of the Amendment prior to examination on the United States Examination Phase.

IN THE CLAIMS:

On amended page 12:

replace line 1 with --WHAT IS CLAIMED IS:--;

Please replace original claims 1-8 with the following rewritten claims 1-8, referring to the mark-ups in Appendix A.

1. (Amended) An authenticating method, comprising the steps of:

carrying out a first operation A(x,g) on a prescribed known value g and on a value x known only to a first entity, said first operation A(x,g) being an asymmetric cryptographic method, thus producing a first operation result;

encoding said first operation result utilizing a first key, which is known to said first and to a second entity, said encoding being carried out with said first key utilizing a symmetrical encoding method, thus producing an encoded first operation result, said first operation result being a second code with which said first entity is authorized to undertake a service on said second entity;

transmitting said encoded first operation result by said first entity to said second entity;

decoding said encoded first operation result by said second entity with said first key, and the first entity is thereby authenticated;

determining said second key in relation to G(gxy), by said second entity carrying out a second operation G(gy) with a secret number y known only to it;

encoding a result of said second operation with said first key; and

transmitting said encoded second operation result to said first entity.

2. (Amended) The method as claimed in claim 1, wherein said first operation A(g,x) is a Diffie-Hellman function (G(gx)), G() being an arbitrary, finite cyclic group G; and said first operation is an RSA function xg.

3. (Amended) The method as claimed in claim 1, wherein said first operation is carried out on a group G selected from the group consisting of:

a) a multiplicative group F_q^* of a finite body F_q, in particular having

- a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p;
- a multiplicative group F_t^* with t = 2m over a finite body F_t of characteristic 2;
- a group of units Z_n^* with n as a composite integer;

b) a group of points on an elliptic curve over a finite body; and

c) a Jacobi variant of a hyperelliptic curve over a finite body.

4. (Amended) The method as claimed in claim 3, wherein said second key is a session key or an authorization associated with an application.

5. (Amended) The method as claimed in claim 1, wherein the Diffie-Hellman method is used to generate said second key.

6. (Amended) The method as claimed in claim 1, wherein said encoding is carried out with said first key utilizing a one-way function.

7. (Amended) The method as claimed in claim 1, wherein said transmitted data are confidential data.

8. (Amended) An authenticating arrangement comprising a processor unit configured to execute the method of claim 1.

Please add the following new claims 9 and 10.

9. (New) The method according to claim 6, wherein said one-way function is a cryptographic one-way function.

10. (New) An authenticating method, comprising the steps of:

carrying out a first operation A(x,g), using a processor of a first entity, on a prescribed known value g and on a value x known only to said first entity, said first operation A(x,g) being an asymmetric cryptographic method, thus producing a first operation result;

encoding said first operation result utilizing a first key, which is known to said first and to a second entity, said encoding being carried out with said first key utilizing a symmetrical encoding method by said processor of said first entity, thus producing an encoded first operation result, said first operation result being a second code with which said first entity is authorized to undertake a service on said second entity;

transmitting said encoded first operation result by said first entity to said second entity via a communication bus connected to said processor of said first entity and connected to a processor of said second entity;

decoding said encoded first operation result by said second entity with said first key using said processor of said second entity, and the first entity is thereby authenticated;

determining said second key in relation to G(gxy), by said second entity carrying out a second operation G(gy) with a secret number y known only to it;

encoding a result of said second operation with said first key; and

transmitting said encoded second operation result to said first entity via said communication bus.

REMARKS

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. Pursuant to 37 CFR 1.125 (b), applicants have concurrently submitted a substitute specification, excluding the claims, and provided a marked-up copy. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment, addition, and/or cancellation of claims is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

Mark Bergner (Reg. No. 45,877)
Mark Bergner
Schiff Hardin & Waite
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473
(312) 258-5779
Attorneys for Applicant

CUSTOMER NUMBER 26574

Appendix A
Mark Ups for Claim Amendments

This redlined draft, generated by CompareRite (TM) - The Instant Redliner, shows the differences between -
original document : Q:\DOCUMENTS\YEAR 2001\P010142\ORIGINAL CLAIMS.DOC
and revised document: Q:\DOCUMENTS\YEAR 2001\P010142\AMENDED CLAIMS.DOC

CompareRite found 47 change(s) in the text

Deletions appear as Overstrike text surrounded by []
Additions appear as Bold-Underline text

1. **(Amended)** An authenticating method, **comprising the steps of:**

carrying [~~a) in which a first entity carries~~] out a first operation A(x,g) on a prescribed known value g and on a value x known only to [~~the~~] **a** first entity, [~~the~~] **said** first operation A(x,g) being an asymmetric cryptographic method**, thus producing a first operation result;**[~~;~~]

[~~b) in which the result of the~~] **encoding said** first operation [~~is encoded with the aid of~~] **result utilizing** a first key, which is known to [~~the~~] **said** first and to a second entity, [~~the~~] **said** encoding being carried out with [~~the~~] **said** first key [~~with the aid of~~] **utilizing** a symmetrical encoding method**, thus producing an encoded first operation result, said**[~~;~~

~~c) in which the result of the~~] first operation [~~encoded with the first key is transmitted by the first entity to the~~] **result being a second code with which said first entity is authorized to undertake a service on said** second entity;

[~~and~~] **transmitting said encoded first operation result by said first entity to said second entity;**

[~~d) in which the result of the first ~~]**decoding said encoded first** operation [~~is decoded~~] **result** by [~~the~~] **said** second entity with [~~the~~] **said** first key, and the first entity is thereby authenticated;

[~~e) in which the result of the first operation is a second code with which the first entity is authorized to undertake a service on the second entity;~~

~~f) in which the second key is determined in relation toG(gxy),~~

~~by virtue of the fact that the second entity carries~~] **determining said second key in relation to G(gxy), by said second entity carrying** out a second operation G(gy) with a secret number y known only to it[~~, encodes the~~]**;**

encoding a result of ~~[this]~~ **said** second operation with ~~[the]~~ **said** first key ~~[and transmits it to the]~~**; and**

transmitting said encoded second operation result to said first entity.

2. **(Amended)** The method as claimed in claim 1, ~~[in which the]~~ **wherein said** first operation A(g,x) [

~~a)~~] is a Diffie-Hellman function (G(gx)**)**, G() being an arbitrary, finite cyclic group G; and **said first operation** ~~[b)]~~ is an RSA function xg.

3. **(Amended)** The method as claimed in ~~[one of the preceding claims, in which the]~~ **claim 1, wherein said** first operation is carried out on a group G[~~,~~] **selected from** the group ~~[G being one of the following groups]~~ **consisting of**:

a) a multiplicative group F_q^* of a finite body F_q, in particular having

a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p;

a multiplicative group F_t^* with t = 2m over a finite body F_t of characteristic 2;

a group of units Z_n^* with n as a composite integer;

b) a group of points on an elliptic curve over a finite body; and

c) a Jacobi variant of a hyperelliptic curve over a finite body.

4. **(Amended)** The method as claimed in ~~[the preceding claim, in which the]~~ **claim 3, wherein said** second key is a session key or an authorization associated with an application.

5. **(Amended)** The method as claimed in ~~[one of the preceding claims, in which]~~ **claim 1, wherein** the Diffie-Hellman method is used to generate ~~[the]~~ **said** second key.

6. **(Amended)** The method as claimed in ~~[one of the preceding claims, in which the]~~ **claim 1, wherein said** encoding is carried out with ~~[the]~~ **said** first key ~~[with the aid of]~~ **utilizing** a one-way function~~[, in particular a cryptographic one-way function.]~~**.**

~~[7.]~~**7. (Amended)** The method as claimed in ~~[one of the preceding claims, in which the]~~ **claim 1, wherein said** transmitted data are confidential data.

8. **(Amended)** An authenticating arrangement [in which] **comprising** a processor unit [is provided which is set up in such a way that a method as claimed in one of the preceding claims can be carried out.] **configured to execute the method of claim 1.**

This redlined draft, generated by CompareRite (TM) - The Instant Redliner, shows the differences between -
original document : Q:\DOCUMENTS\YEAR 2001\P010142\ORIGINAL SPECIFICATION.DOC
and revised document: Q:\DOCUMENTS\YEAR 2001\P010142\SUBSTITUTE SPECIFICATION.DOC

CompareRite found 120 change(s) in the text

Deletions appear as Overstrike text surrounded by []
Additions appear as Bold-Underline text

[~~Description~~] **SPECIFICATION**

[~~Method and arrangement for authenticating a first entity and a second entity~~] **TITLE**

METHOD AND ARRANGEMENT FOR AUTHENTICATING A FIRST ENTITY AND A SECOND ENTITY

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The invention relates to a method and an arrangement for authenticating a first entity with a second entity and/or vice versa.

Description of the Related Art

[0003] During an authentication, a first entity declares to a second entity reliably that it actually is the first entity. There is a corresponding need in the transmission of (confidential) data to ensure from whom [~~said~~] **the** data actually originate.

[0004] A symmetrical encoding method is known from [~~[1]~~] **Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, (Ruland), pages 42-46**. In the symmetric encoding method, a key is used both for the encoding and for the decoding. An attacker who comes into possession of such a key can transform a plain text (the information to be encoded) into encoded text, and vice versa. The symmetrical encoding method is also called private key method or method with a secret key. A known algorithm for symmetrical encoding is the DES (data encryption standard) algorithm. It was standardized in 1974 under ANSI X3.92-1981.

[0005] An asymmetrical encoding method is known from [~~[2]~~] **Ruland, pages 73-85**. In this case, a subscriber is not assigned a single key, but a key system composed of two keys: one key maps the plain text into a transformed one, while the other key permits the inverse operation and converts the transformed text into plain text. Such a method is termed asymmetric[~~,~~] because the two parties participating in a cryptographic operation use different keys (of a key system). One of the two keys, for example a key p, can be made publicly known, if the following properties are fulfilled:

[0006] - It is not possible to derive from the key p with a justifiable outlay**;** a secret key s required for the inverse operation.

[0007] - Even if plain text is transformed with the (public) key p, it is not possible to derive the (secret) key s [~~therefrom.~~

]**from it.**

[0008] For this reason, the asymmetric encoding method is also termed a public key method with a key p which can be made known publicly.

[0009] It is possible in principle to derive the secret key s from the public key p. However, this becomes arbitrarily complicated by virtue of the fact, in particular, that algorithms are selected which are based on problems in complexity theory. These algorithms are also spoken of as “one-way trapdoor” functions. A known representative for an asymmetric encoding method is the Diffie-Hellman method [[~~6~~]] **A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524) (Menezes)**. This method can be used, in particular, for key exchange (Diffie-Hellman key agreement, exponential key exchange).

[0010] The term encoding implies the general application of a cryptographic method V(x,k), in which a prescribed input value x (also termed plain text) is converted by means of a secret k (key) into an encoded text c: = V(x,k). The plain text x can be reconstructed using knowledge of c and k by means of an inverse decoding method. The term encoding is also understood as “one-way encoding” with the property that there is no inverse, efficiently calculable decoding method. Examples of such a one-way encoding method are [

]a cryptographic one-way function or a cryptographic hash function, for example the algorithm SHA-1, see [~~[4].~~

]**NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995, available on-line at http://csrc.nist.gov/fips/fip180-1.ps.**

[0011] There is a problem in practice [~~that it must be ensured~~] **of ensuring** that a public key which is used to verify an electronic signature really is the public key of the person who is assumed to be the originator of the transmitted data (ensuring the authenticity of the originator). The public key therefore need not be kept secret, but it must be authentic. There are known mechanisms (see [~~[3])~~] **Ruland at pages 101-117)** which ensure with a high outlay that the authenticity is reliable. Such a mechanism is the setting up of [~~what is called~~] a trust center, which enjoys trustworthiness and with the aid of which general authenticity is ensured. The setting up of such a trust center, and the exchange of the keys from this trust center are, however, very complicated. For example, it must be ensured during the key allocation that it really is the addressee and not a potential attacker who receives the key or the keys. The costs for setting up and operating the trust center are correspondingly high.

SUMMARY OF THE INVENTION

[0012] It is the object of the invention to ensure authentication[~~, there being no need~~] **without needing** to invest in a separate outlay for a certification entity or a trust center.

[0013] This object is achieved [~~in accordance with the features of the independent patent claims. Developments of the invention follow from the dependent claims.~~] **according to the discussion below.**

[~~In order to achieve the object, a~~]**[0014]** **The inventive** method for [~~authentifying~~] **authenticating** a first entity with a second entity is [~~specified,~~] **provided** in which the first entity [

]carries out an operation A(x,g) on a (publicly) prescribed known value g and on a value x known only to the first entity. The result of the first operation is encoded with the aid of a first key, which is known to the first and second entities. The result of the first operation, encoded by [~~means~~] **way** of the first key, is transmitted by the first entity to the second entity.

[0015] It is particularly advantageous in this case [~~for~~] **to** use [~~to be made of~~] a symmetrical method in order to authenticate one entity in the eyes of a further entity. This authentication is effected without setting up a separate certification entity or a trust center.

[0016] One refinement consists in that the first operation A(x,g) is an asymmetric cryptographic method. In particular, the first operation can be carried out on an arbitrary finite and cyclic group G.

[0017] A further refinement consists in that the first operation A(x,g) is a Diffie-Hellman function G(gx). Alternatively, the first operation can also be an RSA function xg.

[0018] A development consists in that the group G is one of the following groups:

[0019] a) a multiplicative group F_q^* of a finite body F_q, in particular having

[0020] a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p;

[0021] a multiplicative group F_t^* with t = 2m over a finite body F_t of characteristic 2;**and**

[0022] a group of units Z_n^* with n as a composite integer;

[0023] b) a group of points on an elliptic curve over a finite body; and

[0024] c) a Jacobi variant of a hyperelliptic curve over a finite body.

[0025] A further development consists in that the result of the first operation is a second key with which the first entity is authorized to undertake a service on the second entity.

[0026] An additional refinement consists in that the second key is a session key or an authorization associated with an application.

[0027] It also is a development for the second key to be determined in relation to

[0028] G(gxy),

[0029] by virtue of the fact that the second entity carries out an operation G(gy) with a secret number y known only to it. The result of this second operation is encoded with the first key and transmitted to the first entity.

[0030] An additional development consists in that the Diffie-Hellman method is used to generate the second key.

[0031] Another refinement consists in that the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function. A one-way function is distinguished in that it is easy to calculate in one direction, [~~whereas~~] **but** its inversion can be performed only with so large an outlay that [~~this possibility can be neglected in practice~~] **it is impractical**. An example of such a one-way function is a cryptographic hash function which generates an output B from an input A. The output B cannot be used to infer the input A, even when the algorithm of the hash function is known.

[0032] Another development is that the encoding which is carried out with the first key corresponds to a symmetrical encoding method.

[~~Finally, it is a~~]**[0033]** **A final** development **is** that the transmitted data are confidential data.

[0034] Furthermore, to achieve the object, an authenticating arrangement is specified in which a processor unit is provided which is set up in such a way that

[0035] a) a first entity can carry out a first operation A(x,g) on a prescribed known value g and on a value x known only to the first entity;

[0036] b) the result of the first operation can be encoded with the aid of a first key known to the first and to a second entity;

[0037] c) the result of the first operation encoded with the first key can be transmitted by the first entity to the second entity; and

[0038] d) the result of the first operation is decoded by the second entity with the first key, and the first entity can thereby be authenticated.

[0039] This arrangement is particularly suitable for carrying out the method according to the invention or one of its developments explained above.

Brief Description of the Drawings

[0040] Exemplary embodiments of the invention are illustrated and explained below with the aid of the [~~drawing.~~] **drawings.**

[~~In the drawing:~~

~~Fig. 1 shows a sketch~~]**[0041]** **Fig. 1** **is a block diagram** relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case;

[0042] Fig. 2 [~~shows a sketch~~] **is a block diagram** in accordance with fig. 1 and using the DES algorithm; and

[0043] Fig. 3 [~~shows~~] **is a block diagram of** a processor unit.

DETAILED DESCRIPTION OF THE INVENTION

[0044] Fig. 1 is a ~~[sketch]~~ **diagram** relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case. An entity A 101 selects a random number x in a body “mod p-1” (see block 103). The entity 101 now sends an entity 102 a message 104 which has the following format:

[0045] g, p, T_A, ID_A, gx mod p, H(g^x mod p, ~~[PW]~~ **pw**, ID_A, T_A, ...),

[0046] where

x denotes a secret random value of the entity A 101,

y denotes a secret random value of the entity B 102,

g denotes a generator according to the Diffie-Hellman method,

p denotes a prime number for the Diffie-Hellman method,

T_A denotes a time stamp of the entity A during generation and/or transmission of the message,

T_B denotes a time stamp of the entity B during generation and/or transmission of the message,

ID_A denotes an identification feature of the entity A,

ID_B denotes an identification feature of the entity B,

g^x mod p denotes a public Diffie-Hellman key of the entity A,

g^y mod p denotes a public Diffie-Hellman key of the entity B,

~~[PW]~~ **pw** denotes a shared secret between the entities A and B (password “shared secret”),

H(M) denotes a cryptographic one-way function (hash function) over the parameters M, and

~~[KEY]~~ **key** denotes a session key common to the two entities A and B.

[0047] If this message has arrived at the entity 102, a random number y is selected there (see block 105) from the body “mod p-1” and a common key is agreed **to** in a block 106 as

~~[KEY]~~**[0048]** **key** = g^{xy} mod p.

[0049] The second entity 102 transmits a message 107 with the format

[0050] TB, ID_B, g^y mod p, H(g^y mod p, ~~[PW]~~ **pw**, ID_B, T_B, ...)

[0051] to the first entity 101. The first entity 101 will ~~[thereupon]~~ **then** carry out the operation

~~[KEY]~~**[0052]** **key** = g^{xy} mod p

[0053] in a step 108, this likewise yielding the common key ~~[KEY.]~~**“key”.**

~~[It may be pointed out expressly in]~~**[0054]** **In** this case ~~[that]~~, for example, the body "mod p-1" has been selected as one of many possibilities. Furthermore, the messages 104 and 107 are ~~[to be]~~ regarded in each case as one possibility of many. In particular, the fields for addressing within the messages depend on the application and/or the transmission protocol used.

[0055] A cryptographic one-way hash function H is used in ~~[fig]~~ **Fig**. 1. An example for transmitting such a one-way hash function is the SHA-1 algorithm (compare ~~[[4])]~~ **NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; available on-line at http://csrc.nist.gov/fips/fip180-1.ps)**. The use of a symmetrical encoding method, for example the DES algorithm ~~[[5]]~~ **NIST, FIPS PUB 81: DES Modes of Operation, December 1980; available on-line at http://www.itl.nist.gov/div897/pubs/fip81.htm**, instead of the one-way hash function H, is illustrated in ~~[fig]~~ **Fig**. 2. The blocks 101, 102, 103, 105, 106 and 108 are identical in ~~[fig.]~~ **Fig.** 2 to ~~[fig. 1]~~ **Fig. 1**. The message 201 transmitted by the first entity 101 to the second entity 102 has the format

[0056] g, p, T_A, ID_A, g^x mod p, ~~[ENCPW(gx]~~ **Encr$_{PW}$(g^x** mod p, ~~[PW]~~ **pw**, ID_A, T_A, ...),

[0057] where

~~[ENCPW(M)]~~**[0058]** **Encr$_{PW}$(M)** denotes a symmetrical method for encoding the parameter M with the key PW.

[0059] In the reverse direction, the entity 102 sends the entity 101 in fig. 2 the message 202 which has the following format:

[0060] TB, ID_B, g^y mod p, ~~[ENCPW(gy]~~ **Encr$_{PW}$(g^y** mod p, PW, IDB, TB, ...).

~~[It may be remarked here, in particular, that in]~~**[0061]** **In** each case**,** one message (the message 104 in ~~[fig]~~ **Fig**. 1, and the message 201 in ~~[fig]~~ **Fig**. 2) suffices in order to authenticate the first entity 101 with respect to the second entity ~~[202]~~ **102**. Disregarding the fact that the second entity 102, for example**,** a service to be undertaken within a network connection~~[,]~~ **(**for example the Internet~~[,]~~**)** must also be authenticated, it can suffice if only the first entity 101 is authenticated. This already ~~[obtains]~~ **derives** after transmission of the respective first messages 104 and 201. If, in particular, the first entity 101 dials in at the second entity 102, it is frequently to be assumed that this second entity 102 is also the correct entity. Conversely, the second entity 102 must be able to assume that the caller (the first entity 101) is also the one for which it is outputting. Checking authenticity is therefore important in this direction, from the first entity 101 to the second entity 102.

[0062] Fig. 3 illustrates a processor unit PRZE. The processor unit PRZE comprises a processor CPU, a memory SPE and an input/output interface IOS which ~~[is]~~ **are** used in various ways via an interface IFC. Via a graphics interface, an output is visualized on a monitor MON and/or output on a printer PRT. An input is performed via a mouse MAS or a keyboard TAST. The processor unit PRZE also has a data bus BUS, which ensures the connection of a memory MEM, the processor CPU**,** and the input/output interface IOS. Furthermore, additional components, for example**,** additional memory, data memory (hard disk) or scanner, can be connected to the data bus BUS.

~~[List of references:]~~**[0063]** **The above-described method and arrangement are illustrative of the principles of the present invention. Numerous modifications and adaptations will be**

readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.

[~~[1] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 42-46.~~] **ABSTRACT**

~~[[2] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 73-85.~~

~~[3] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 101-117.~~

~~[4] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; http://csrc.nist.gov/fips/fip180-1.ps~~

~~[5] NIST, FIPS PUB 81: DES Modes of Operation, December 1980; http://www.itl.nist.gov/div897/pubs/fip81.htm~~

~~[6] A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524).~~

~~Abstract~~

~~Method and arrangement for authenticating a first entity and a second entity~~

]**[0064]** In order to authenticate a first entity at a second entity, a first number is generated by ~~[means]~~ **way** of an asymmetric cryptographic method. This first number is symmetrically encoded and transmitted to the second entity. The second entity checks the first number by decoding the second number and thereby authenticates the first entity.

SPECIFICATION

TITLE

METHOD AND ARRANGEMENT FOR AUTHENTICATING A FIRST ENTITY AND A SECOND ENTITY

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The invention relates to a method and an arrangement for authenticating a first entity with a second entity and/or vice versa.

Description of the Related Art

[0002] During an authentication, a first entity declares to a second entity reliably that it actually is the first entity. There is a corresponding need in the transmission of (confidential) data to ensure from whom the data actually originate.

[0003] A symmetrical encoding method is known from Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, (Ruland), pages 42-46. In the symmetric encoding method, a key is used both for the encoding and for the decoding. An attacker who comes into possession of such a key can transform a plain text (the information to be encoded) into encoded text, and vice versa. The symmetrical encoding method is also called private key method or method with a secret key. A known algorithm for symmetrical encoding is the DES (data encryption standard) algorithm. It was standardized in 1974 under ANSI X3.92-1981.

[0004] An asymmetrical encoding method is known from Ruland, pages 73-85. In this case, a subscriber is not assigned a single key, but a key system composed of two keys: one key maps the plain text into a transformed one, while the other key permits the inverse operation and converts the transformed text into plain text. Such a method is termed asymmetric because the two parties participating in a cryptographic operation use different keys (of a key system). One of the two keys, for example a key p, can be made publicly known, if the following properties are fulfilled:

[0005] - It is not possible to derive from the key p with a justifiable outlay; a secret key s required for the inverse operation.

[0006] - Even if plain text is transformed with the (public) key p, it is not possible to derive the (secret) key s from it.

[0007] For this reason, the asymmetric encoding method is also termed a public key method with a key p which can be made known publicly.

[0008] It is possible in principle to derive the secret key s from the public key p. However, this becomes arbitrarily complicated by virtue of the fact, in particular, that algorithms are selected which are based on problems in complexity theory. These algorithms are also spoken of as "one-way trapdoor" functions. A known representative for an asymmetric encoding method is the Diffie-Hellman method A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524) (Menezes). This method can be used, in particular, for key exchange (Diffie-Hellman key agreement, exponential key exchange).

[0009] The term encoding implies the general application of a cryptographic method V(x,k), in which a prescribed input value x (also termed plain text) is converted by means of a secret k (key) into an encoded text c: = V(x,k). The plain text x can be reconstructed using knowledge of c and k by means of an inverse decoding method. The term encoding is also understood as "one-way encoding" with the property that there is no inverse, efficiently calculable decoding method. Examples of such a one-way encoding method are a cryptographic one-way function or a cryptographic hash function, for example the algorithm SHA-1, see NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995, available on-line at http://csrc.nist.gov/fips/fip180-1.ps.

[0010] There is a problem in practice of ensuring that a public key which is used to verify an electronic signature really is the public key of the person who is assumed to be the originator of the transmitted data (ensuring the authenticity of the originator). The public key therefore need not be kept secret, but it must be authentic. There are known mechanisms (see Ruland at pages 101-117) which ensure with a high outlay that the authenticity is reliable. Such a mechanism is the setting up of a trust center, which enjoys trustworthiness and with the aid of which general authenticity is ensured. The setting up of such a trust center, and the exchange of the keys from this trust center are, however, very complicated. For example, it must be ensured during the key allocation that it really is the addressee and not a potential attacker who receives the key or the keys. The costs for setting up and operating the trust center are correspondingly high.

SUMMARY OF THE INVENTION

[0011] It is the object of the invention to ensure authentication without needing to invest in a separate outlay for a certification entity or a trust center.

[0012] This object is achieved according to the discussion below.

[0013] The inventive method for authenticating a first entity with a second entity is provided in which the first entity carries out an operation A(x,g) on a (publicly) prescribed known value g and on a value x known only to the first entity. The result of the first operation is encoded with the aid of a first key, which is known to the first and second entities. The result of the first operation, encoded by way of the first key, is transmitted by the first entity to the second entity.

[0014] It is particularly advantageous in this case to use a symmetrical method in order to authenticate one entity in the eyes of a further entity. This authentication is effected without setting up a separate certification entity or a trust center.

[0015] One refinement consists in that the first operation A(x,g) is an asymmetric cryptographic method. In particular, the first operation can be carried out on an arbitrary finite and cyclic group G.

[0016] A further refinement consists in that the first operation A(x,g) is a Diffie-Hellman function G(gx). Alternatively, the first operation can also be an RSA function xg.

[0017] A development consists in that the group G is one of the following groups:

[0018] a) a multiplicative group $\mathbb{F}_q^*$ of a finite body $\mathbb{F}_q$, in particular having

[0019] a multiplicative group $\mathbb{Z}_p^*$ of the integers modulo of a prescribed prime number p;

[0020] a multiplicative group $\mathbb{F}_t^*$ with t = 2m over a finite body $\mathbb{F}_t$ of characteristic 2; and

[0021] a group of units Z_n^* with n as a composite integer;

[0022] b) a group of points on an elliptic curve over a finite body; and

[0023] c) a Jacobi variant of a hyperelliptic curve over a finite body.

[0024] A further development consists in that the result of the first operation is a second key with which the first entity is authorized to undertake a service on the second entity.

[0025] An additional refinement consists in that the second key is a session key or an authorization associated with an application.

[0026] It also is a development for the second key to be determined in relation to

[0027] G(gxy),

[0028] by virtue of the fact that the second entity carries out an operation G(gy) with a secret number y known only to it. The result of this second operation is encoded with the first key and transmitted to the first entity.

[0029] An additional development consists in that the Diffie-Hellman method is used to generate the second key.

[0030] Another refinement consists in that the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function. A one-way function is distinguished in that it is easy to calculate in one direction, but its inversion can be performed only with so large an outlay that it is impractical. An example of such a one-way function is a cryptographic hash function which generates an output B from an input A. The output B cannot be used to infer the input A, even when the algorithm of the hash function is known.

[0031] Another development is that the encoding which is carried out with the first key corresponds to a symmetrical encoding method.

[0032] A final development is that the transmitted data are confidential data.

[0033] Furthermore, to achieve the object, an authenticating arrangement is specified in which a processor unit is provided which is set up in such a way that

[0034] a) a first entity can carry out a first operation A(x,g) on a prescribed known value g and on a value x known only to the first entity;

[0035] b) the result of the first operation can be encoded with the aid of a first key known to the first and to a second entity;

[0036] c) the result of the first operation encoded with the first key can be transmitted by the first entity to the second entity; and

[0037] d) the result of the first operation is decoded by the second entity with the first key, and the first entity can thereby be authenticated.

[0038] This arrangement is particularly suitable for carrying out the method according to the invention or one of its developments explained above.

Brief Description of the Drawings

[0039] Exemplary embodiments of the invention are illustrated and explained below with the aid of the drawings.

[0040] Fig. 1 is a block diagram relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case;

[0041] Fig. 2 is a block diagram in accordance with fig. 1 and using the DES algorithm; and

[0042] Fig. 3 is a block diagram of a processor unit.

DETAILED DESCRIPTION OF THE INVENTION

[0043] Fig. 1 is a diagram relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case. An entity A 101 selects a random number x in a body "mod p-1" (see block 103). The entity 101 now sends an entity 102 a message 104 which has the following format:

[0044] g, p, T_A, ID_A, gx mod p, H(g^x mod p, pw, ID_A, T_A, ...),

[0045] where

x denotes a secret random value of the entity A 101,

y denotes a secret random value of the entity B 102,

g denotes a generator according to the Diffie-Hellman method,

p denotes a prime number for the Diffie-Hellman method,

T_A denotes a time stamp of the entity A during generation and/or transmission of the message,

T_B denotes a time stamp of the entity B during generation and/or transmission of the message,

ID_A denotes an identification feature of the entity A,

ID_B denotes an identification feature of the entity B,

g^x mod p denotes a public Diffie-Hellman key of the entity A,

g^y mod p denotes a public Diffie-Hellman key of the entity B,

pw denotes a shared secret between the entities A and B (password “shared secret”),

H(M) denotes a cryptographic one-way function (hash function) over the parameters M, and

key denotes a session key common to the two entities A and B.

[0046] If this message has arrived at the entity 102, a random number y is selected there (see block 105) from the body “mod p-1” and a common key is agreed to in a block 106 as

[0047] key = g^{xy} mod p.

[0048] The second entity 102 transmits a message 107 with the format

[0049] TB, ID_B, g^y mod p, H(g^y mod p, pw, ID_B, T_B, ...)

[0050] to the first entity 101. The first entity 101 will then carry out the operation

[0051] key = g^{xy} mod p

[0052] in a step 108, this likewise yielding the common key “key”.

[0053] In this case, for example, the body “mod p-1” has been selected as one of many possibilities. Furthermore, the messages 104 and 107 are regarded in each case as one possibility of many. In particular, the fields for addressing within the messages depend on the application and/or the transmission protocol used.

[0054] A cryptographic one-way hash function H is used in Fig. 1. An example for transmitting such a one-way hash function is the SHA-1 algorithm (compare [0001]

NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; available on-line at http://csrc.nist.gov/fips/fip180-1.ps). The use of a symmetrical encoding method, for example the DES algorithm NIST, FIPS PUB 81: DES Modes of Operation, December 1980; available on-line at http://www.itl.nist.gov/div897/pubs/fip81.htm, instead of the one-way hash function H, is illustrated in Fig. 2. The blocks 101, 102, 103, 105, 106 and 108 are identical in Fig. 2 to Fig. 1. The message 201 transmitted by the first entity 101 to the second entity 102 has the format

[0055] g, p, T_A, ID_A, g^x mod p, $Encr_{PW}(g^x \text{ mod } p, pw, ID_A, T_A, ...)$,

[0056] where

[0057] $Encr_{PW}(M)$ denotes a symmetrical method for encoding the parameter M with the key PW.

[0058] In the reverse direction, the entity 102 sends the entity 101 in fig. 2 the message 202 which has the following format:

[0059] TB, ID_B, g^y mod p, $Encr_{PW}(g^y \text{ mod } p, PW, IDB, TB, ...)$.

[0060] In each case, one message (the message 104 in Fig. 1, and the message 201 in Fig. 2) suffices in order to authenticate the first entity 101 with respect to the second entity 102. Disregarding the fact that the second entity 102, for example, a service to be undertaken within a network connection (for example the Internet) must also be authenticated, it can suffice if only the first entity 101 is authenticated. This already derives after transmission of the respective first messages 104 and 201. If, in particular, the first entity 101 dials in at the second entity 102, it is frequently to be assumed that this second entity 102 is also the correct entity. Conversely, the second entity 102 must be able to assume that the caller (the first entity 101) is also the one for which it is outputting. Checking authenticity is therefore important in this direction, from the first entity 101 to the second entity 102.

[0061] Fig. 3 illustrates a processor unit PRZE. The processor unit PRZE comprises a processor CPU, a memory SPE and an input/output interface IOS which are used in various ways via an interface IFC. Via a graphics interface, an output is visualized on a monitor MON and/or output on a printer PRT. An input is performed via a mouse MAS or a keyboard TAST. The processor unit PRZE also has a data bus BUS, which ensures the connection of a memory MEM, the processor CPU, and the input/output interface IOS. Furthermore, additional components, for example, additional memory, data memory (hard disk) or scanner, can be connected to the data bus BUS.

[0062] The above-described method and arrangement are illustrative of the principles of the present invention. Numerous modifications and adaptations will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.

ABSTRACT

[0063] In order to authenticate a first entity at a second entity, a first number is generated by way of an asymmetric cryptographic method. This first number is symmetrically encoded and transmitted to the second entity. The second entity checks the first number by decoding the second number and thereby authenticates the first entity.

Description

Method and arrangement for authenticating a first entity and a second entity

The invention relates to a method and an arrangement for authenticating a first entity with a second entity and/or vice versa.

During an authentification, a first entity declares to a second entity reliably that it actually is the first entity. There is a corresponding need in the transmission of (confidential) data to ensure from whom said data actually originate.

A symmetrical encoding method is known from [1]. In the symmetric encoding method, a key is used both for the encoding and for the decoding. An attacker who comes into possession of such a key can transform a plain text (the information to be encoded) into encoded text, and vice versa. The symmetrical encoding method is also called private key method or method with a secret key. A known algorithm for symmetrical encoding is the DES (data encryption standard) algorithm. It was standardized in 1974 under ANSI X3.92-1981.

An asymmetrical encoding method is known from [2]. In this case, a subscriber is not assigned a single key, but a key system composed of two keys: one key maps the plain text into a transformed one, while the other key permits the inverse operation and converts the transformed text into plain text. Such a method is termed asymmetric, because the two parties participating in a cryptographic operation use different keys (of a key system). One of the two keys, for example a key p, can be made publicly known, if the following properties are fulfilled:

- It is not possible to derive from the key p with a justifiable outlay a secret key s required for the inverse operation.
- Even if plain text is transformed with the (public) key p, it is not possible to derive the (secret) key s therefrom.

For this reason, the asymmetric encoding method is also termed a public key method with a key p which can be made known publicly.

It is possible in principle to derive the secret key s from the public key p. However, this becomes arbitrarily complicated by virtue of the fact, in particular, that algorithms are selected which are based on problems in complexity theory. These algorithms are also spoken of as "one-way trapdoor" functions. A known representative for an asymmetric encoding method is the Diffie-Hellman method [6]. This method can be used, in particular, for key exchange (Diffie-Hellman key agreement, exponential key exchange).

The term encoding implies the general application of a cryptographic method V(x,k), in which a prescribed input value x (also termed plain text) is converted by means of a secret k (key) into an encoded text c: = V(x,k). The plain text x can be reconstructed using knowledge of c and k by means of an inverse decoding method. The term encoding is also understood as "one-way encoding" with the property that there is no inverse, efficiently calculable decoding method. Examples of such a one-way encoding method are a cryptographic one-way function or a cryptographic hash function, for example the algorithm SHA-1, see [4].

There is a problem in practice that it must be ensured that a public key which is used to verify an electronic signature really is the public key of the person who is assumed to be the originator of the transmitted data (ensuring the authenticity of the originator). The public key therefore need not be kept secret, but it must be authentic. There are known mechanisms (see [3]) which ensure with a high outlay that the authenticity is reliable. Such a mechanism is the setting up of what is called a trust center, which enjoys trustworthiness and with the aid of which general authenticity is ensured. The setting up of such a trust center, and the exchange of the keys from this trust center are, however, very complicated. For example, it must be ensured during the key allocation that it really is the addressee and not a potential attacker who receives the key or the keys. The costs for setting up and operating the trust center are correspondingly high.

It is the **object** of the invention to ensure authentication, there being no need to invest in a separate outlay for a certification entity or a trust center.

This object is achieved in accordance with the features of the independent patent claims. Developments of the invention follow from the dependent claims.

In order to achieve the object, a method for authentifying a first entity with a second entity is specified, in which the first entity carries out an operation $A(x,g)$ on a (publicly) prescribed known value g and on a value x known only to the first entity. The result of the first operation is encoded with the aid of a first key, which is known to the first and second entities. The result of the first operation, encoded by means of the first key, is transmitted by the first entity to the second entity.

It is particularly advantageous in this case for use to be made of a symmetrical method in order to authenticate one entity in the eyes of a further entity. This authentication is effected without setting up a separate certification entity or a trust center.

One refinement consists in that the first operation $A(x,g)$ is an asymmetric cryptographic method. In particular, the first operation can be carried out on an arbitrary finite and cyclic group G.

A further refinement consists in that the first operation $A(x,g)$ is a Diffie-Hellman function $G(g^x)$. Alternatively, the first operation can also be an RSA function x^g.

A development consists in that the group G is one of the following groups:

a) a multiplicative group F_q^* of a finite body F_q, in particular having
   - a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p;
   - a multiplicative group F_t^* with $t = 2^m$ over a finite body F_t of characteristic 2;
   - a group of units Z_n^* with n as a composite integer;

b) a group of points on an elliptic curve over a finite body; and

c) a Jacobi variant of a hyperelliptic curve over a finite body.

A further development consists in that the result of the first operation is a second key with which the first entity is authorized to undertake a service on the second entity.

An additional refinement consists in that the second key is a session key or an authorization associated with an application.

It also is a development for the second key to be determined in relation to

$$G(g^{xy}),$$

by virtue of the fact that the second entity carries out an operation $G(g^{y})$ with a secret number y known only to it. The result of this second operation is encoded with the first key and transmitted to the first entity.

An additional development consists in that the Diffie-Hellman method is used to generate the second key.

Another refinement consists in that the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function. A one-way function is distinguished in that it is easy to calculate in one direction, whereas its inversion can be performed only with so large an outlay that this possibility can be neglected in practice. An example of such a one-way function is a cryptographic hash function which generates an output B from an input A. The output B cannot be used to infer the input A, even when the algorithm of the hash function is known.

Another development is that the encoding which is carried out with the first key corresponds to a symmetrical encoding method.

Finally, it is a development that the transmitted data are confidential data.

Furthermore, to achieve the object, an authenticating arrangement is specified in which a processor unit is provided which is set up in such a way that

a) a first entity can carry out a first operation A(x,g) on a prescribed known value g and on a value x known only to the first entity;

b) the result of the first operation can be encoded with the aid of a first key known to the first and to a second entity;

c) the result of the first operation encoded with the first key can be transmitted by the first entity to the second entity; and

d) the result of the first operation is decoded by the second entity with the first key, and the first entity can thereby be authenticated.

This arrangement is particularly suitable for carrying out the method according to the invention or one of its developments explained above.

Exemplary embodiments of the invention are illustrated and explained below with the aid of the drawing.

In the drawing:

Fig. 1 shows a sketch relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case;

Fig. 2 shows a sketch in accordance with fig. 1 and using the DES algorithm; and

Fig. 3 shows a processor unit.

Fig. 1 is a sketch relating to the agreement of a common key between two entities whose respective authenticity is ensured in each case. An entity A 101 selects a random number x in a body "mod p-1" (see block 103). The entity 101 now sends an entity 102 a message 104 which has the following format:

$$g, p, T_A, ID_A, g^x \bmod p, H(g^x \bmod p, PW, ID_A, T_A, \ldots),$$

where

x denotes a secret random value of the entity A 101,

y denotes a secret random value of the entity B 102,

g denotes a generator according to the Diffie-Hellman method,

p denotes a prime number for the Diffie-Hellman method,

T_A denotes a time stamp of the entity A during generation and/or transmission of the message,

T_B denotes a time stamp of the entity B during generation and/or transmission of the message,

ID_A denotes an identification feature of the entity A,

ID_B denotes an identification feature of the entity B,

$g^x \bmod p$ denotes a public Diffie-Hellman key of the entity A,

$g^y \bmod p$ denotes a public Diffie-Hellman key of the entity B,

PW denotes a shared secret between the entities A and B (password "shared secret"),

H(M) denotes a cryptographic one-way function (hash function) over the parameters M, and

KEY denotes a session key common to the two entities A and B.

If this message has arrived at the entity 102, a random number y is selected there (see block 105) from the body "mod p-1" and a common key is agreed in a block 106 as

$$KEY = g^{xy} \bmod p.$$

The second entity 102 transmits a message 107 with the format

$$T_B,\ ID_B,\ g^y \bmod p,\ H(g^y \bmod p,\ PW,\ ID_B,\ T_B,\ \ldots)$$

to the first entity 101. The first entity 101 will thereupon carry out the operation

$$KEY = g^{xy} \bmod p$$

in a step 108, this likewise yielding the common key KEY.

It may be pointed out expressly in this case that, for example, the body "mod p-1" has been selected as one of many possibilities. Furthermore, the messages 104 and 107 are to be regarded in each case as one possibility of many. In particular, the fields for addressing within the messages depend on the application and/or the transmission protocol used.

A cryptographic one-way hash function H is used in fig. 1. An example for transmitting such a one-way hash function is the SHA-1 algorithm (compare [4]). The use of a symmetrical encoding method, for example the DES algorithm [5], instead of the one-way hash function H, is illustrated in **fig. 2.** The blocks 101, 102, 103, 105, 106 and 108 are identical in fig. 2 to fig. 1. The message 201 transmitted by the first entity 101 to the second entity 102 has the format

$$g,\ p,\ T_A,\ ID_A,\ g^x \bmod p,\ ENC_{PW}(g^x \bmod p,\ PW,\ ID_A,\ T_A,\ \ldots),$$

where

$ENC_{PW}(M)$ denotes a symmetrical method for encoding the parameter M with the key PW.

In the reverse direction, the entity 102 sends the entity 101 in fig. 2 the message 202 which has the following format:

$$T_B,\ ID_B,\ g^y \bmod p,\ ENC_{PW}(g^y \bmod p,\ PW,\ ID_B,\ T_B,\ \ldots).$$

It may be remarked here, in particular, that in each case one message (the message 104 in fig. 1, and the message 201 in fig. 2) suffices in order to authenticate the first entity 101 with respect to the second entity 202. Disregarding the fact that the second entity 102, for example a service to be undertaken within a network connection, for example the Internet, must also be authenticated, it can suffice if only the first entity 101 is authenticated. This already obtains after transmission of the respective first messages 104 and 201. If, in particular, the first entity 101 dials in at the second entity 102, it is frequently to be assumed that this second entity 102 is also the correct entity. Conversely, the second entity 102 must be able to assume that the caller (the first entity 101) is also the one for which it is outputting. Checking authenticity is therefore important in this direction, from the first entity 101 to the second entity 102.

Fig. 3 illustrates a processor unit PRZE. The processor unit PRZE comprises a processor CPU, a memory SPE and an input/output interface IOS which is used in various ways via an interface IFC. Via a graphics interface, an output is visualized on a monitor MON and/or output on a printer PRT. An input is performed via a mouse MAS or a keyboard TAST. The processor unit PRZE also has a data bus BUS, which ensures the connection of a memory MEM, the processor CPU and the input/output interface IOS. Furthermore, additional components, for example additional memory, data memory (hard disk) or scanner, can be connected to the data bus BUS.

List of references:

[1] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 42-46.

[2] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 73-85.

[3] Christoph Ruland: Informationssicherheit in Datennetzen [Information security in data networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, pages 101-117.

[4] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; http://csrc.nist.gov/fips/fip180-1.ps

[5] NIST, FIPS PUB 81: DES Modes of Operation, December 1980; http://www.itl.nist.gov/div897/pubs/fip81.htm

[6] A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524).

Patent claims

1. An authenticating method,

a) in which a first entity carries out a first operation A(x,g) on a prescribed known value g and on a value x known only to the first entity, the first operation A(x,g) being an asymmetric cryptographic method;

b) in which the result of the first operation is encoded with the aid of a first key, which is known to the first and to a second entity, the encoding being carried out with the first key with the aid of a symmetrical encoding method;

c) in which the result of the first operation encoded with the first key is transmitted by the first entity to the second entity; and

d) in which the result of the first operation is decoded by the second entity with the first key, and the first entity is thereby authenticated;

e) in which the result of the first operation is a second code with which the first entity is authorized to undertake a service on the second entity;

f) in which the second key is determined in relation to

$G(g^{xy})$,

by virtue of the fact that the second entity carries out a second operation $G(g^{y})$ with a secret number y known only to it, encodes the result of this second operation with the first key and transmits it to the first entity.

2. The method as claimed in claim 1, in which the first operation A(g,x)

a) is a Diffie-Hellman function (G(g^x), G() being an arbitrary, finite cyclic group G; and

b) is an RSA function x^g.

3. The method as claimed in one of the preceding claims, in which the first operation is carried out on a group G, the group G being one of the following groups:

a) a multiplicative group F_q^* of a finite body F_q, in particular having
   - a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p;
   - a multiplicative group F_t^* with $t = 2^m$ over a finite body F_t of characteristic 2;
   - a group of units Z_n^* with n as a composite integer;

b) a group of points on an elliptic curve over a finite body; and

c) a Jacobi variant of a hyperelliptic curve over a finite body.

4. The method as claimed in the preceding claim, in which the second key is a session key or an authorization associated with an application.

5. The method as claimed in one of the preceding claims, in which the Diffie-Hellman method is used to generate the second key.

6. The method as claimed in one of the preceding claims, in which the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function.

7. The method as claimed in one of the preceding claims, in which the transmitted data are confidential data.

8. An authenticating arrangement in which a processor unit is provided which is set up in such a way that a method as claimed in one of the preceding claims can be carried out.

GR 98 P 2998

Abstract

Method and arrangement for authenticating a first entity and a second entity

In order to authenticate a first entity at a second entity, a first number is generated by means of an asymmetric cryptographic method. This first number is symmetrically encoded and transmitted to the second entity. The second entity checks the first number by decoding the second number and thereby authenticates the first entity.

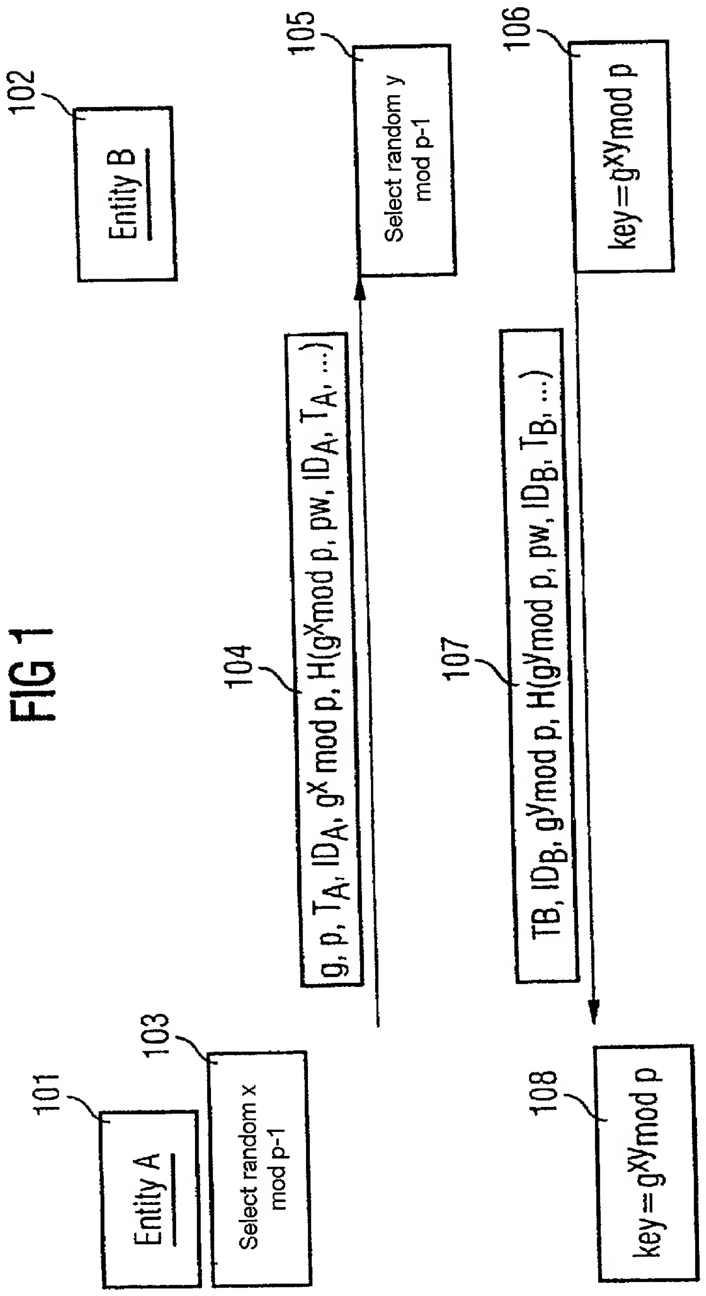


FIG 1

101
Entity A
102
Entity B
103
Select random x mod p-1
104
g, p, T_A, ID_A, g^x mod p, H(g^x mod p, pw, ID_A, T_A, ...)
105
Select random y mod p-1
106
key=g^xy mod p
107
TB, ID_B, g^y mod p, H(g^y mod p, pw, ID_B, T_B, ...)
108
key=g^xy mod p

FIG 2

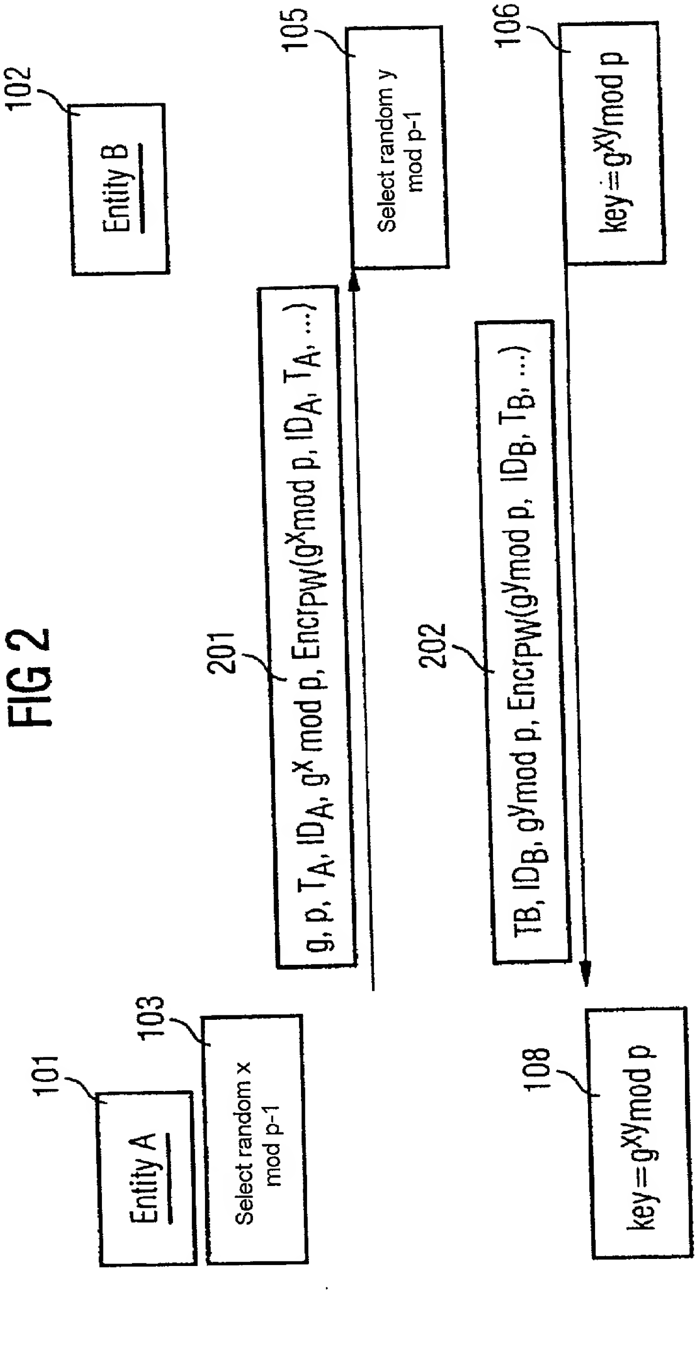
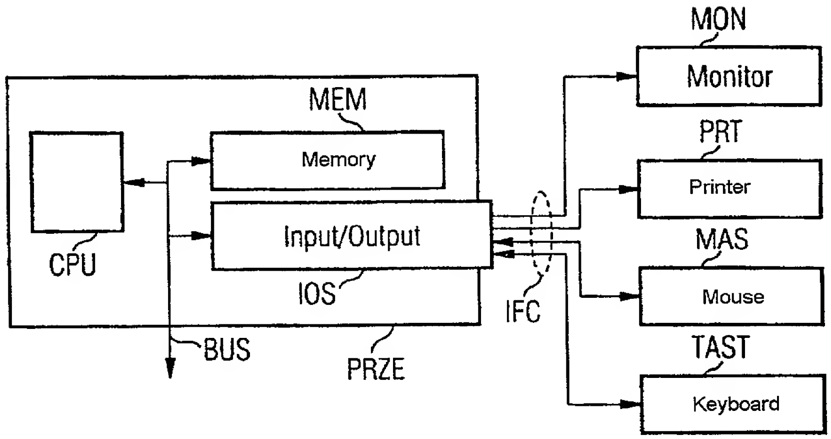

Entity B
102
Select random y mod p-1
105
key=g^xy mod p
106
g, p, T_A, ID_A, g^x mod p, Encrpw(g^x mod p, ID_A, T_A, ...)
201
TB, ID_B, g^y mod p, Encrpw(g^y mod p, ID_B, T_B, ...)
202
Entity A
101
Select random x mod p-1
103
key=g^xy mod p
108

FIG 3


MON
Monitor
MEM
Memory
PRT
Printer
Input/Output
CPU
IOS
MAS
Mouse
IFC
TAST
BUS
PRZE
Keyboard

Declaration and Power of Attorney For Patent Application

Erklärung Für Patentanmeldungen Mit Vollmacht

German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

Verfahren und Anordnung zur Authentifikation von einer ersten Instanz und einer zweiten Instanz

deren Beschreibung

(zutreffendes ankreuzen)

□ hier beigefügt ist.

☒ am 11.10.1999 als PCT internationale Anmeldung

PCT Anmeldungsnummer PCT/DE99/03262

eingereicht wurde und am ________ abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Method and array for authenticating a first instance and a second instance

the specification of which

(check one)

□ is attached hereto.

☒ was filed on 11.10.1999 as PCT international application

PCT Application No. PCT/DE99/03262

and was amended on ________
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign appplications
Prioritát beansprucht

			Priority Claimed	
19850665.1	DE	03.11.1998	☒	□
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			□	□
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			□	□
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

PCT/DE99/03262	11.10.1999		
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date D, M, Y) (Anmeldedatum T, M, J)	(Status) (patentiert, anhängig, aufgegeben)	(Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date D,M,Y) (Anmeldedatum T, M; J)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

And I hereby appoint

Customer No. 26574

Telefongespräche bitte richten an:
(Name und Telefonnummer)

Direct Telephone Calls to: *(name and telephone number)*

Ext. ________________

Postanschrift:

Send Correspondence to:

Schiff, Hardin & Waite
6600 Sears Tower 60606-6473 Chicago, Illinois
Telephone: +1 312 258 5780 and Facsimile +1 312 258 5921
~~or~~
Customer No. 26574

Voller Name des einzigen oder ursprünglichen Erfinders: MARTIN EUCHNER	Full name of sole or first inventor: MARTIN EUCHNER
Unterschrift des Erfinders Datum Martin Euchner 26.3.2001	Inventor's signature Date
Wohnsitz MUENCHEN, DEUTSCHLAND DEX	Residence MUENCHEN, GERMANY
Staatsangehorigkeit DE	Citizenship DE
Postanschrift LORENZSTR. 2	Post Office Addess LORENZSTR. 2
81737 MUENCHEN	81737 MUENCHEN
Voller Name des zweiten Miterfinders (falls zutreffend):	Full name of second joint inventor, if any:
Unterschrift des Erfinders Datum	Second Inventor's signature Date
Wohnsitz ,	Residence ,
Staatsangehorigkeit	Citizenship
Postanschrift	Post Office Address

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).